

CLAIMS

1. Method of transferring data from a non-volatile memory (24) to a working memory (22) of an electronic data processing device (10), comprising the steps
5 of:
copying data from the non-volatile memory to the working memory, which data includes security data (30) to be write-protected, (steps 36; 50, 58),
activating a blocking of the security data in the working memory, (step 38; 52),
monitoring all communication with the working memory, (steps 34, 42; 56),
10 and
blocking all write attempts to the copied security data stored in the working memory, (steps 44; 60),
wherein at least the steps of activating a blocking, monitoring communication and blocking write attempts are performed independently of the central
15 processing unit (14) of the data processing device, such that the central processing unit cannot manipulate the security data.
2. Method according to claim 1, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in a device for blocking
20 write attempts (16) and used at least in relation to activating a blocking.
3. Method according to claim 1 or 2, wherein the step of copying data comprises copying only the security data from the non-volatile memory to the working
25 memory independently of the central processing unit of the data processing device (step 50) and copying any further data under the control of the central processing unit of the device (step 58).
4. Method according to claim 3, wherein the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data
30 in the working memory are pre-defined and wherein the step of activating a blocking of positions of the working memory is triggered by the copying being made to the pre-defined area in the working memory and the blocking is activated for said area.
- 35 5. Method according to claim 1 or 2, wherein the step of copying comprises copying all data from the non-volatile memory to the working memory under the control of the central processing unit of the device (step 36).

- 5 6. Method according to claim 5, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and wherein the step of activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and the blocking is activated for that area of the working memory.
- 10 7. Method according to any previous claim, wherein the step of blocking is achieved by changing the destination address of the data transferred to the working memory.
- 15 8. Method according to any previous claim, further comprising the steps of disconnecting a debugging unit (step 32; 48) at least when copying the security data to the working memory and reconnecting the debugging unit (step 40; 54) when the blocking has been activated.
- 20 9. Device (16) for blocking write attempts to security data (30) transferred from a non-volatile memory (24) to a working memory (22) in an electronic data processing environment (10) that includes a central processing unit (14) and comprising a monitoring unit (28) arranged to:
activate a blocking of the security data in the working memory upon copying of the security data from the non-volatile memory to the working memory,
monitor all communication with the working memory, and
block all write attempts to the copied security data stored in the working memory,
25 all performed independently of the central processing unit of the data processing environment such that the central processing unit cannot manipulate the security data.
- 30 10. Device according to claim 9, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in the device and used in relation at least to activating a blocking.
- 35 11. Device according to claim 9 or 10, further comprising a copy control unit (46) arranged to copy the security data from the non-volatile memory to the working memory also independently of the central processing unit of the data processing environment.
12. Device according to claim 11, where the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data

in the working memory are pre-defined and pre-stored in the device and the monitoring unit when activating a blocking is triggered by the copying being made to the pre-defined area in the working memory and activates a blocking of that area.

5

13. Device according to claim 9 or 10, where the area of the security data (A1, A2) in the non-volatile memory is pre-defined and pre-stored in the device and the monitoring unit when activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and activating a blocking for that area of the working memory.

10

14. Device according to any of claims 9 – 13, wherein the monitoring unit is arranged to block write attempts by changing the destination address of data transferred to the working memory.

15

15. Device according to any of claims 9 – 14, wherein the monitoring unit is arranged to disconnect a debugging unit (26) of the electronic data processing environment at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.

20

16. Device according to any of claims 9 – 15, wherein it is implemented in hardware.

25

17. Electronic data processing device (10) comprising:
a non-volatile memory (24) comprising data including security data (30) to be write-protected,
a working memory (22),
a central processing unit (14) arranged to control copying of at least some data from the non-volatile memory to the working memory, and
a device for blocking write attempts (16) to security data transferred from the non-volatile memory to the working memory and comprising a monitoring unit (28) arranged to:
activate a blocking of the security data in the working memory upon copying of the security data from the non-volatile memory to the working memory,
monitor all communication with the working memory, and
block all write attempts to the copied security data stored in the working memory,

30

35

all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data.

- 5 18. Electronic data processing device according to claim 17, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and used in relation at least to activating a blocking.
- 10 19. Electronic data processing device according to claim 17 or 18, wherein the device for blocking write attempts further comprises a copy control unit (46) arranged to copy the security data from the non-volatile memory to the working memory independently of the central processing unit and the central processing unit is arranged to control the copying of further data from the non-volatile memory to the working memory.
- 15 20. Electronic data processing device according to claim 19, where the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data in the working memory are pre-defined and pre-stored in the device for blocking write attempts and the monitoring unit when
- 20 activating a blocking is triggered by the copying being made to the pre-defined area in the working memory and activates a blocking of that area.
- 25 21. Electronic data processing device according to claim 17 or 18, wherein the central processing unit is arranged to control the copying of all data from the non-volatile memory to the working memory.
- 30 22. Electronic data processing device according to claim 21, where the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and the monitoring unit when activating a blocking is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and activating a blocking for that area of the working memory.
- 35 23. Electronic data processing device according to any of claims 17 – 22, wherein the monitoring unit is arranged to block write attempts by changing the destination address of data transferred to the working memory.

24. Electronic data processing device according to any of claims 17 – 23, further comprising a debugging unit (26) and wherein the monitoring unit is arranged to disconnect the debugging unit at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.
25. Electronic data processing device according to any of claims 17 – 24, wherein the device for blocking write attempts is implemented in hardware.
26. Electronic data processing device according to any of claims 17 – 25, wherein the device is a portable communication device.
27. Electronic data processing device according to claim 26, wherein the device is a cellular phone.